Patent
Attorney Docket No. 030681-291

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of
A-jung Kim
Application No.: 09/816,080
Filing Date: March 26, 2001
Group Art Unit: 2135
Examiner: BEEMNET DADA
Confirmation No.: 7143
Title: KEY AGREEMENT METHOD IN SECURE COMMUNICATION SYSTEM USING MULTIPLE ACCESS METHOD

AMENDMENT/REPLY TRANSMITTAL LETTER

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Enclosed is a reply for the above-identified patent application.

☐ A Petition for Extension of Time is also enclosed.

☐ Terminal Disclaimer(s) and the ☐ $55.00 (2814) ☐ $110.00 (1814) fee per Disclaimer due under 37 C.F.R. § 1.20(d) are also enclosed.

☐ Also enclosed is/are _____

☐ Small entity status is hereby claimed.

☐ Applicant(s) requests continued examination under 37 C.F.R. § 1.114 and enclose the ☐ $395.00 (2801) ☐ $790.00 (1801) fee due under 37 C.F.R. § 1.17(e).

☐ Applicant(s) requests that any previously unentered after final amendments not be entered. Continued examination is requested based on the enclosed documents identified above.

☐ Applicant(s) previously submitted _____
on _____,
for which continued examination is requested.

☐ Applicant(s) requests suspension of action by the Office until at least _____, which does not exceed three months from the filing of this RCE, in accordance with 37 C.F.R. § 1.103(c). The required fee under 37 C.F.R. § 1.17(i) is enclosed.

☐ A Request for Entry and Consideration of Submission under 37 C.F.R. § 1.129(a) (1809/2809) is also enclosed.

☒ No additional claim fee is required.

☐ An additional claim fee is required, and is calculated as shown below.

AMENDED CLAIMS					
	No. of Claims	**Highest No. of Claims Previously Paid For**	**Extra Claims**	**Rate**	**Additional Fee**
Total Claims		MINUS =	0	x $18.00 (1202) =	$ 0.00
Independent Claims		MINUS =	0	x $88.00 (1201) =	$ 0.00
If Amendment adds multiple dependent claims, add $300.00 (1203)					
Total Claim Amendment Fee					$ 0.00
☐ Small Entity Status claimed - subtract 50% of Total Claim Amendment Fee					$ 0.00
TOTAL ADDITIONAL CLAIM FEE DUE FOR THIS AMENDMENT					**$ 0.00**

☐ A check in the amount of _____ is enclosed for the fee due.

☐ Charge _____ to Deposit Account No. 02-4800.

☐ Charge _____ to credit card. Form PTO-2038 is attached.

The Director is hereby authorized to charge any appropriate fees under 37 C.F.R. §§ 1.16, 1.17, 1.20(d) and 1.21 that may be required by this paper, and to credit any overpayment, to Deposit Account No. 02-4800. This paper is submitted in duplicate.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

By _____
Charles F. Wieland III
Registration No. 33,096

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

Date: October 14, 2004

Patent
Attorney's Docket No. 030681-291

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
A-jung Kim	Group Art Unit: 2135
Application No.: 09/816,080	Examiner: BEEMNET DADA
Filed: March 26, 2001	Confirmation No.: 7143
For: KEY AGREEMENT METHOD IN SECURE COMMUNICATION SYSTEM USING MULTIPLE ACCESS METHOD	

REQUEST FOR RECONSIDERATION

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In reply to the Office Action of July 14, 2004, Applicants respectfully request reconsideration of the above-captioned application.

The Office Action includes a rejection of claims 1-6 under 35 U.S.C. § 103 as allegedly being unpatentable over the Lo et al. patent (U.S. Patent 5,732,139) in view of the Mazourenko et al. patent (U.S. Patent 6,272,224). This rejection is respectfully traversed.

The Lo et al. Patent

The Lo et al. patent relates to a quantum cryptographic system having a method for distributing at random cryptographic keys using quantum mechanics to reduce data loss. In columns 5 and 6, it addresses a prior art technique for two users, traditionally called Alice and Bob, to share a secret random key that can

subsequently be used to send meaningful secret messages when needs arise. Alice and Bob use a quantum channel to send polarized photons and another "classical public channel" to send messages. Alice and Bob use the public channel to discuss and compare signals sent through the quantum channel in order to test them for evidence of eavesdropping or other errors. Errors can occur, as discussed at column 6, beginning at line 18, due to either intrinsic noise of the channel or eavesdropping attack by a third party, traditionally called Eve. That identifies with the prior art technology Alice and Bob choose *randomly* m photons from the ones that are transmitted and received in the same basis. For each of the m photons, Bob announces publicly his measurement result. Alice tells Bob publicly whether his result is the same as which he originally prepared. For this, an error rate can be computed and if it exceeds a predetermined tolerable error rate then it can be inferred that the channel is either noisy or substantial eavesdropping has occurred. A similar disclosure occurs at column 8, lines 54-60.

It is respectfully submitted that the description of the Lo et al. patent in the Office Action is not completely correct. Specifically, it identifies that the second user adopts only bits having measured value beyond a threshold value, which is predetermined, citing the above passages for support. However, it is clear from a second reading of these passages that the bits are chosen randomly, and not with reference to a threshold value.

The Mazourenko et al. Patent

The Mazourenko et al. patent discloses a process and device for quantum distribution of an encryption key. It operates by modulating a light beam with a signal, the phase of which can be adjusted at random. On reception, the received beam is modulated by a signal, the phase of which is also adjustable. The intensity of one of the lateral modes is measured, which depends on the difference between the two phases used. The key is transmitted by the photons and contained in one of the lateral modes.

The Office cites the Mazourenko et al. patent as allegedly teaching a method of key distribution wherein the second user informs the first user of the bits adopted in the nth bits that are transmitted in a bit sequence and not telling of the value of the bits citing column 4, lines 37-41 and column 8, lines 54-67.

The Hypothetical Combination

It is respectfully submitted that one of ordinary skill in the art would not have found it obvious to combine the Mazourenko et al. key distribution method with the Lo et al. cryptographic system. As characterized in the Office Action, the Mazourenko et al. method does not inform the sender of the bits the values of the bits. However, this is in bright contrast to the Lo et al. system, which depends upon a measurement result being transmitted back to the sender. Hence, the adoption of the Mazourenko et al. technique in the Lo et al. system would appear to render that system inoperative. The same would be true if the roles were reversed insofar as the Mazourenko et al. patent appears to depend on the revelation of the phase that

he used in detecting the bits from a sender. Hence, Applicants respectfully submit that the primary and secondary references are not properly combinable insofar as their combination would appear to render either one or the other one inoperative for its stated purpose. See, In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).

Additionally, it is respectfully submitted that the hypothetical combination would not achieve the combination of features found in claim 1. As pointed out before, claim 1 recites that the second user adopts only bits having a measured value beyond the threshold value which is predetermined. This is found in neither of the applied references, and, hence, the hypothetical combination would not meet the recitations of independent claim 1.

The Lo et al. patent also describes a prior art quantum key distribution scheme which involves Alice generating and sending Bob a sequence of photons whose polarizations she has chosen at random to be one of four different polarizations. For each photon received, Bob measures its polarization along either a rectilinear or diagonal basis with equal probability. Bob announces publicly, for each photon, which basis is chosen but not the measurement result. Alice tells Bob publicly, for each photon, whether he has made his measurement result along the correct basis. Thereafter, Alice and Bob then discard all cases in which Bob has made the measurement along the wrong basis and keep only the ones that Bob has made the measurement along the correct basis. See column 5, lines 36-55.

The Mazourenko et al. patent, in describing the quantum distribution of encryption keys, describes the process at the destination end at column 6,

particularly step e), as including a photodetector receiving one of lateral modes, the signal output for this photodetector depending on the phase difference between the first phase shift chosen by the sender and the second phase shift chosen by the addressee and step f), the sender then informs which photons were detected, through a public channel, but without revealing the values of the second phase shift used. See column 6, lines 14-21.

The present invention concerns a key arrangement method including a first system which encodes a bit sequence and sends it to a second system. The second system decodes the received signals and measures the signal values. The second system records some second values, which are above a predetermined value, and tells the first system bit positions of the selected bits. The first system selects values corresponding to those bit positions and discards the rest of them. In comparing the present invention to the Lo et al. patent, a measurement target of the present invention is, as shown in Fig. 4 and described at the last paragraph of page 6, for instance, a signal value, in contrast to the polarization of the photon as measured by the Lo et al. system. The second system decides key positions and informs the first system of them, in accordance with the present invention. In contrast, in the Lo et al. patent, the second measures and informs the first side of the measurement basis, and keeps the measurements based on the correct measurement type. Hence, the present invention differs from the Lo et al. patent in that in the Lo et al. patent, the second side measures values and the first side is involved in the key decision. It is the receiving system, or second system, that decides keys in the present invention.

Regarding the Mazourenko et al. patent, a measurement target is phase difference, as described above. Hence, it is respectfully submitted that neither the Lo et al. nor the Mazourenko et al. patent disclose the present invention as it is described in the pending claims.

Dependent claims 2-6 further separate the present invention from the applied art but the additional distinctions will not be belabored for sake of brevity.

In light of the foregoing, Applicants respectfully request reconsideration and allowance of the above-captioned application. Should any residual issues exist, the Examiner is invited to contact the undersigned at the number listed below.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: October 14, 2004

By: _____
Charles F. Wieland III
Registration No. 33,096

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620